



**DEPARTMENT OF THE NAVY**

BUREAU OF MEDICINE AND SURGERY  
2300 E STREET NW  
WASHINGTON DC 20372-5300

IN REPLY REFER TO

**BUMEDINST 5510.8**

**BUMED-912**

**7 Jan 2002**

**BUMED INSTRUCTION 5510.8**

**From:** Chief, Bureau of Medicine and Surgery  
**To:** All Internal BUMED Codes

**Subj:** EMERGENCY ACTION PLAN FOR PROTECTION OF CLASSIFIED MATERIAL  
AND SECURE TELEPHONE UNITS

**Ref:** (a) OPNAVINST 5510.60L  
(b) SECNAVINST 5510.36  
(c) CMS 6

**Encl:** (1) Emergency Action Plan  
(2) Emergency Procedures for COMSEC Material  
(3) Emergency Procedures for Classified Information

1. Purpose. To establish procedures to protect classified and communications security (COMSEC) material during emergency situations such as a natural disaster or civil disturbance.

2. Responsibility. The command security manager is responsible for the coordination and implementation of this plan and for the accuracy of this instruction. However, management and security of classified and COMSEC material responsibilities are at all levels of the command. Assistant chiefs and special assistants are responsible for the management of classified material within their department and the training of department personnel in the proper procedures for handling and storing classified material. Assistant chiefs shall have an emergency action plan for each space where classified material is used or stored. A copy of each plan will be submitted to the security manager.

3. General. The possibility of unauthorized access to classified and COMSEC material is increased during times of emergency. This plan is to protect publications and equipment from compromise during civil uprising, mob actions, natural disaster, riot, terrorism, and enemy action. Enclosures (1) through (3) list the procedures for action. The importance of ensuring the security of publications and equipment assigned to the communications security system becomes paramount in an emergency, and is the primary responsibility of every holder of COMSEC. References (a) through (c) provide further guidance.

4. Secure Telephone Unit (STU III) COMSEC Equipment. This equipment is located in Chief, Bureau of Medicine and Surgery's office, Building 1, room 1112, the Readiness Division, Building 3, room 3000, and the Telecommunication Center, Building 1, room 1005. This is a specially designed telephone terminal that is capable of retaining COMSEC keying material. The terminals may be used in a network with other terminals.

BUMEDINST 5510.8

7 Jan 2002

5. Points of Contact. The COMSEC material systems (CMS) custodian is Naval Computer and Telecommunications Station Washington, Washington Navy Yard at (202) 433-7840 or the CMS alternate custodian is Bureau of Medicine and Surgery, Security Division, Washington DC at (202) 762-3308.

A handwritten signature in black ink, appearing to read 'D. C. Arthur', with a long horizontal flourish extending to the right.

D. C. ARTHUR

Deputy

Available at: <https://bumed.med.navy.mil/instructions/internal/internal.htm>

## EMERGENCY ACTION PLAN

1. Natural Disaster (flood, earthquake, etc.). Actions taken during a natural disaster will be directed at securing and protecting the classified material. It may become necessary to remove the classified material to a more secure location. In case removal of classified material from work area becomes necessary, deliver the classified material to the Security Office located in Building 5, room 5218.

2. Hostile Action (enemy attack, mob actions or civil uprising). Actions taken in the event of hostile action will be directed at keeping classified/cryptographic material from falling into the control of enemy forces/rioters. If possible, the same actions for natural disaster will be taken. However, it may become necessary to implement the emergency destruction plan.

### a. Emergency Destruction

(1) Emergency destruction will be implemented only as a last resort to avoid losing control of classified material in an instance of imminent enemy takeover.

(2) Upon receipt of orders to initiate emergency destruction, classified material will be destroyed in order of sensitivity.

(3) All classified paper material (messages, files, publications, etc.) will be carried through the fire exit to the nearest dumpster and burned.

(4) Destruction of equipment will be accomplished by using axes, sledge hammers, etc. Equipment will be totally destroyed so that reconstruction is impossible. If complete destruction becomes impractical due to time constraints, the most sensitive components of the equipment (e.g., disk drives) will be destroyed.

### b. Fire Emergency Procedures in a Space Containing Classified Material

(1) Secure all classified material in designated containers if time permits.

(2) Important considerations in case of fire in a secure space.

(a) Safety of personnel first.

(b) Prevention of damage to cryptographic material while maintaining physical security.

(c) Preservation of as much of the classified material as possible.

(d) Removal and protection of classified material, if at all possible, without endangering personnel.

7 Jan 2002

- (e) Continual observation of area until re-entry can be effected.
- (f) Make a list of all unclear fire fighters that enter the space.
- (g) Record the type of material that was left in view and extent of unauthorized viewing.
- (h) Report of possible compromise, due to unauthorized viewing or unexplained loss, will be submitted.

3. Reports

- a. Report all incidences of suspected compromised classified materials.
- b. Report all materials and equipment that are destroyed.
- c. Precautionary destruction priorities list, for COMSEC material is listed in enclosure (2).

4. STU III COMSEC Equipment. This equipment is located in Chief, Bureau of Medicine and Surgery's office, Building 1, room 1112, (202) 762-1643, the Readiness Division, Building 3, room 3000, (202) 762-3437, and the Telecommunication Center, Building 1, room 1005, (202) 762-3312. This is a specially designed telephone terminal that is capable of retaining COMSEC keying material. The terminals may be used in a network with other terminals.

5. Points of Contact. The CMS custodian is Naval Computer and Telecommunications Station Washington, Washington Navy Yard at (202) 433-7840 or the CMS alternate is Bureau of Medicine and Surgery, Security Division, Washington DC at (202) 762-3308.

7 Jan 2002

**EMERGENCY PROCEDURES FOR COMSEC MATERIAL**

1. Reference (c) established procedures to ensure no COMSEC publications and equipment will be compromised due to a civil uprising, mob actions, natural disaster, riot, terrorism, and enemy action. The importance of ensuring the security of publications and equipment assigned to Communications Security System become paramount in an emergency, and is the primary responsibility of every holder of CMS material.
2. In the case of an emergency, the command's Secure Telephone Unit (STU III) must be protected to avoid compromising COMSEC material.
3. In an emergency situation in which the Command is evacuated, users must make every attempt to bring the Crypto Ignition Keys (CIKs) and await further instructions from the STU III COMSEC account (SCA) or CMS custodian and/or alternate.
  - a. CIK holders must always take their CIKs with them in case of emergency.
  - b. If time does not permit or power prohibits zeroizing the terminals, remove the terminal, and take it with you if possible.
  - c. Physically destroy the terminal in extreme emergencies for the following conditions: terrorism and enemy attack or any other emergencies which can cause grave damage to the United States Government by physically smashing terminal with heavy instrument (e.g., hammer, ax, etc.)
    - (1) Burn or break to prevent unauthorized use.
    - (2) Destroy any classified account records and reports.

Enclosure (2)

7 Jan 2002

**EMERGENCY PROCEDURES FOR CLASSIFIED INFORMATION**

Security measures will not endanger the health or safety of personnel. In the event of natural disaster, fire, flood, or some other natural disaster/hostile action enemy attack, mob action, civil disturbance, or terrorist attack, which could result in a possible compromise of classified material, immediate action will be taken to protect classified material from unauthorized personnel. In all instances, the protection of classified information will be implemented in a manner, which will minimize the risk of loss of life or injury to personnel.

1. There are three basic methods of disposition that must be followed according to the type of emergency:

a. Securing. Classified material will be stored only in approved storage containers that satisfy the requirements of reference (a). If the area must be evacuated, a complete inventory shall be taken upon return to the area to determine what, if any material is missing.

b. Removing. In the event of fire, natural disaster, major civil riot, or other emergency situations, it may become necessary for classified and COMSEC material to be removed and placed at the Naval Computer and Telecommunications Station, Washington Navy Yard, Washington DC where physical security can be maintained. The security manager and the staff CMS officers must know the location of the material at all times. If removal is required, a complete inventory of all COMSEC material will be prepared and submitted to the security manager. The security manager will ensure required debriefing procedures are in place as required.

c. Destroying. Destroying the material should be considered as a last alternative. All reasonable efforts should be made to secure or remove the material. If an emergency destruction is ordered, methods of destruction are: Destroy all "SECRET" material first, followed by "Confidential" and "For Official Use Only (FOUO)."

(1) Shredding. Classified material may be shredded in a crosscut shredder that shreds no greater than 3/64 inch wide by 1/2 inch long, however, it may complement burning when practicable.

(2) Burning. This is a primary method of destruction due to location of the incinerator at the Pentagon, Washington DC; classified material may be placed in the brown and red striped bags and delivered to the Security Office located in Building 5, room 5218.

(3) Microfiche. Shredding does not completely destroy microfiche. Therefore, classified microfiche must be destroyed by burning or erasing with an acetone solution (e.g., nail polish remover).

2. When reporting emergency destruction, accurate information concerning the extent of the emergency destruction of classified material is second only in importance to the destruction of the material itself. The facts surrounding the destruction will be reported to the security

Enclosure (3)

7 Jan 2002

manager, who will in turn compile and report all pertinent facts, by the most expeditious means available, to the Chief of Naval Operations (CNO) (N09N2). Reports will contain the following information:

- a. Identification of the items of classified material that may not have been destroyed.
- b. Information concerning classified material which may be presumed to have been destroyed.
- c. Identification of all classified material destroyed and the methods of destruction.